

KEK GRID CA

Takashi Sasaki

KEK Computing Research Center



Who we are?

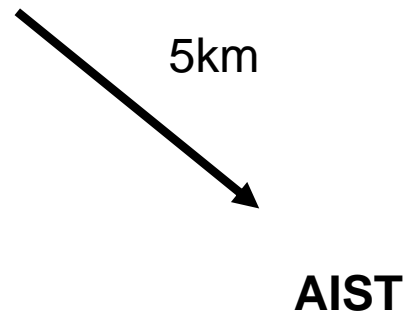
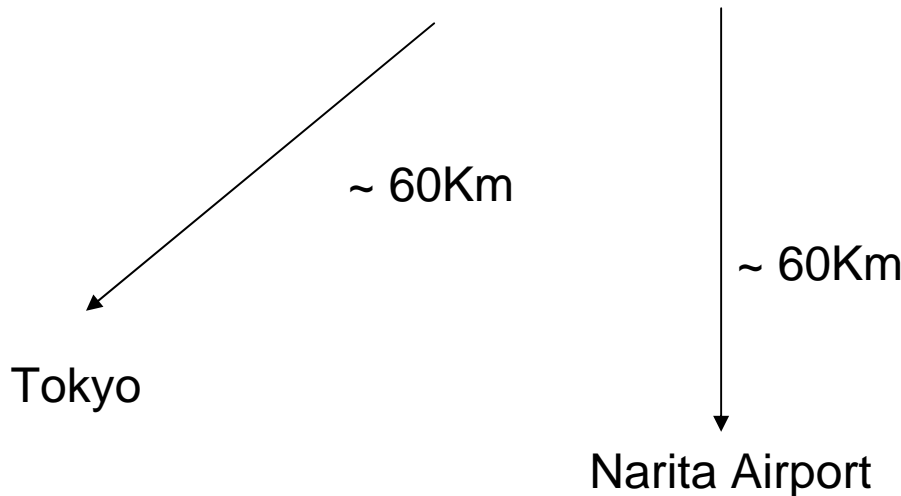
- KEK stands for
 - Kou = High
 - Enerugi = Energy
 - Kasokuki kennkyuu kikou = Accelerator Research Organization
- In Tsukuba city as well as AIST
- Former National Laboratory and Inter University Research Organization since 2003 due to government reorganization





KEKB Accelerator
1km diameter ring
injector etc
Photon factory
Proton synchrotron

~40Km
J-PARC
New Proton Synchrotron
Joint venture with JAERI



KEK Computing Research Center

- We are responsible for
 - Deployment and operation of computing facilities and network in KEK
 - One of the biggest super computer center in Japan
 - New blue gene will be delivered in March and will be the fastest in Japan and 4th in TOP500
 - Belle computing system will be replaced in March
 - 2500 CPU with 2.5 PB storage
 - Central computer system will be replaced in February
 - HPSS
 - GRID
 - Research and development related computing in accelerator science including application software
 - GRID, simulation and etc.



KEK GRID CA

- The production CA will make a service for
 - KEK employees
 - Collaborators of KEK
- Most of them are users of LCG
 - ATLAS Japan
 - Belle
 - Computing Research Center R&D



Experimental CA

- Running since one year ago
 - 261 certificates issued in total
 - 15 are revoked among them
 - Mostly server certificates
 - 10 subscribers
- Based on in house software
 - With the web interface
- We asked Dr. Tanaka at AIST to review the CP/CPS of this system and he found many problems
 - We decided to introduce new one



Production CA (to be)

- Based on the NAREGI CA software
 - No secret key will be not transmit over the network
 - We will use the username/password instead of one time password (license ID)
- Equipped with **FIPS 140-2 Level 3** security module
 - nCipher nShield 1500
- No certificates are issued yet for the users, but test purpose only



Machine Room

- The CA room is inside the computing center building in KEK
 - The building entrances are protected by electrical key in the night and holidays
- The CA space is inside one of the machine rooms
 - The machine room door is locked 24hours and only CRC staffs can open
 - The CA space is protected by steel shutter with the lock and used for CA dedicatedly
 - Only allowed persons can enter in this space
 - Log notes for singning enter/leave in/from the space

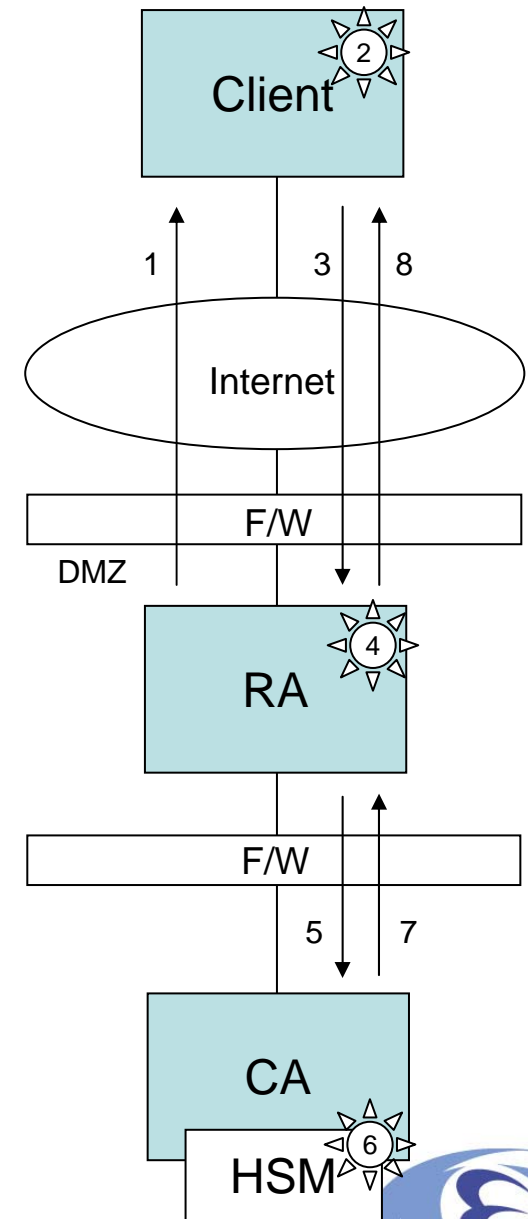


KEK GRID CA System Certificate Request Procedure

* KEK GRID CA base on NAREGI-CA software

1. All users have to download client toolkit from RA Web, and install into their machines.
2. Users can create private key and certificates signing request (CSR) on their client machine using client toolkit or Web browser extension (Internet Explorer only)
3. Users send to CSR to RA server
4. RA server identify and verify users, and then accept users' CSR.
5. RA forward CSR to CA
6. CA signs and publish new certificate with its private key, protected by HSM
7. CA return signed certificate to RA.
8. RA returns published signed certificate to user.

* *All network connection encrypted with SSL



KEK GRID CA System Detail

- CA Server & RA Server
 - IBM eServer xSeries 226
 - Intel Xeon 3GHz Processor
 - 1GB DDR2 Main Memory
 - 73GB SCSI HDD x 2 (RAID-1)
 - Recordable DVD drive for data backup
 - 2 IBM PC servers are prepared
 - NAREGI-CA runs on these machines
 - one is dedicated to CA function and the other one is dedicated to RA function.
 - A UPS supply a power
- Hardware Security Module
 - nCipher nShield 1500
 - protects CA's private key
 - The key is only activated with Smart Card slotted in.
 - HSM is connected to CA machine via PCI bus.
 - CA software contact HSM with using PKCS#11 API.
 - Supports **FIPS 140-2 Level 3** security level.

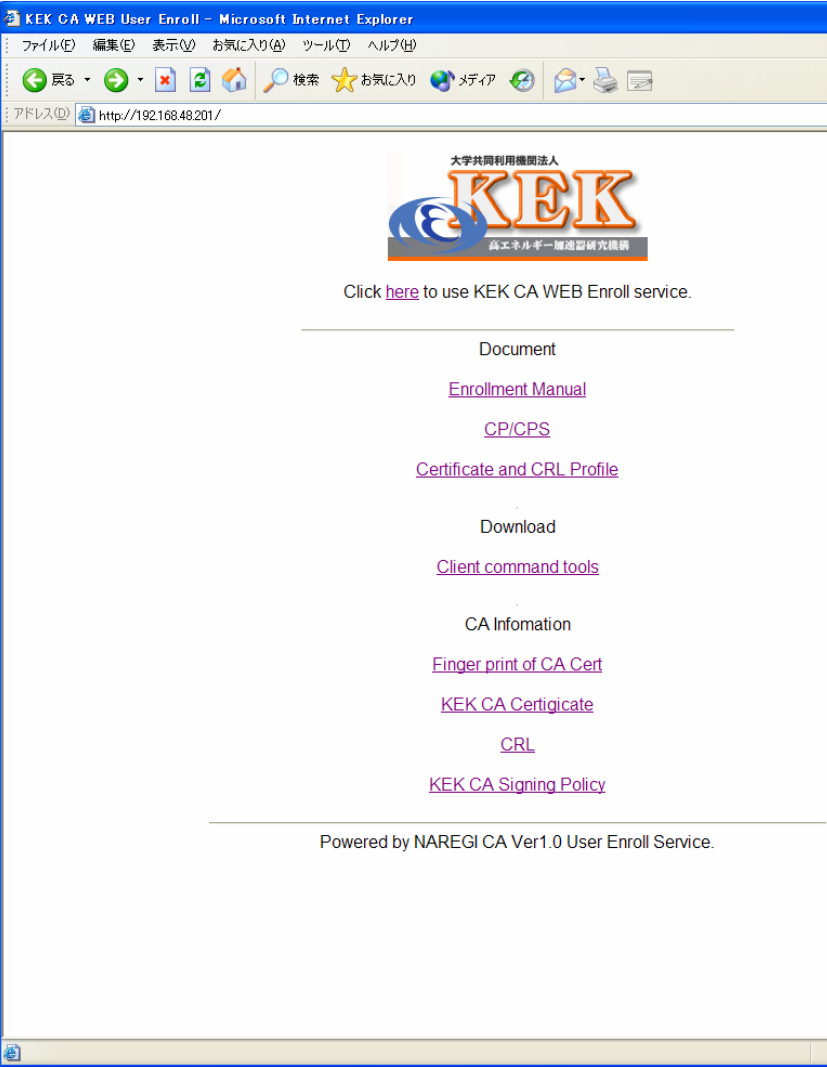


Event records and archives (followed AIST)

- CA system logs
 - Access and operation logs to the CA daemon process
 - Error logs for accesses and operations to the CA daemon process
 - Operation logs of the CA daemon process
- RA system logs
 - Access and operation logs to the RA daemon process
 - Error logs for accesses and operations to the RA daemon process
 - Logs of issued certificates
 - All issued CRLs
 - The date of issuance of CRLs
- Unix system logs
 - shutdown/boot/reboot logs of the CA server and the RA server
 - login/logout/sudo logs of the CA and the RA server
 - other logs archived by UNIX operating of the CA and the RA server
- Logs of physical access to the CA room
 - Paper sheets which record all events about the access to the CA space.
- Emails
 - All emails received by the KEK GRID CA and RA
 - All emails of system-logs sent from the CA and the RA servers
- Other documents
 - A list of email addresses of end entities
 - All issued certificates
 - for each approved request, how the request was approved
 - for each rejected request, how the request was rejected
 - official documents if they are used for identification of entities
 - All versions of the CP/CPS
 - All versions of the Certificate and CRL Profile
 - Internal documents for the operation of KEK GRID CA
 - All Audit reports in the future



Web enrollment



KEK CA WEB User Enroll - Microsoft Internet Explorer

http://192.168.48.201/

大学共同利用機関法人
KEK
高エネルギー加速器研究機構

Click [here](#) to use KEK CA WEB Enroll service.

Document

- [Enrollment Manual](#)
- [CP/CPS](#)
- [Certificate and CRL Profile](#)

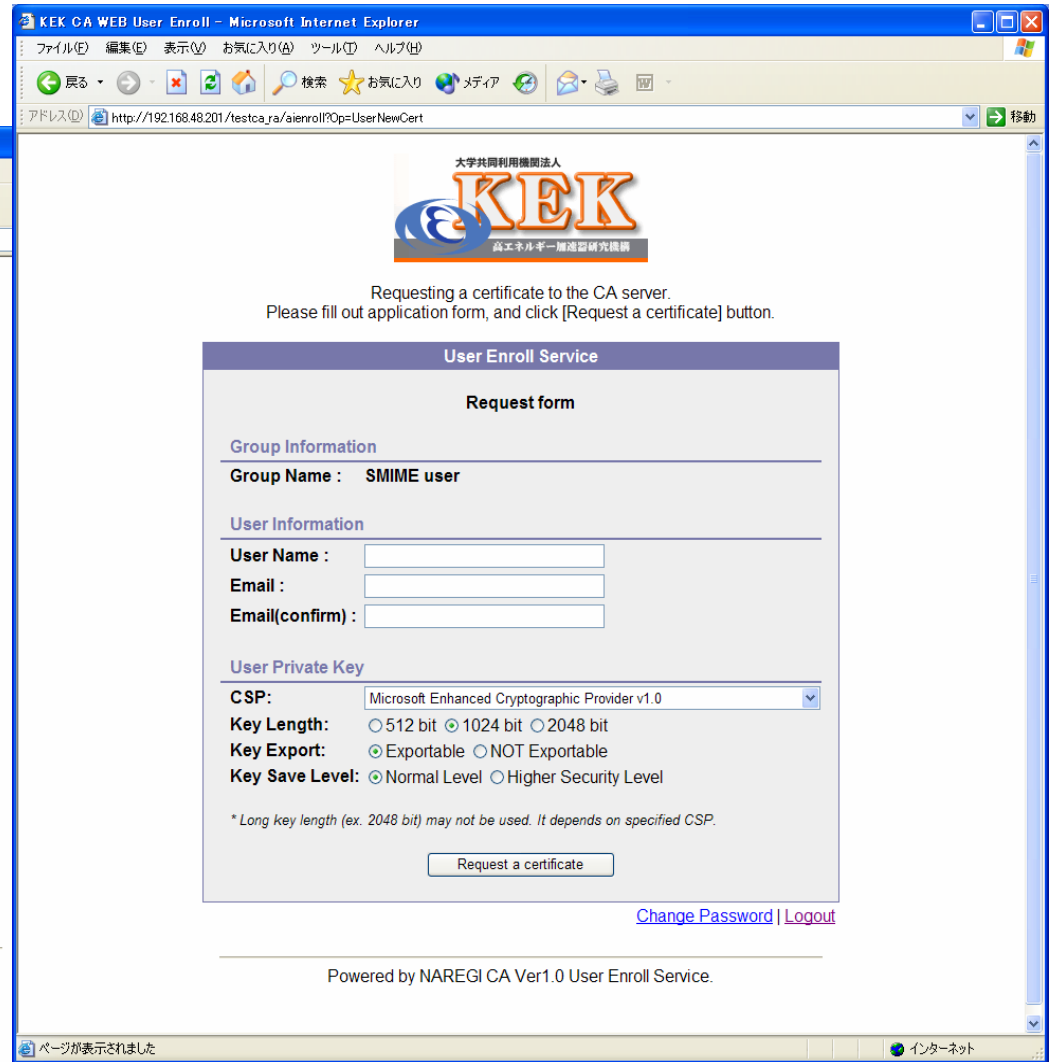
Download

- [Client command tools](#)

CA Information

- [Finger print of CA Cert](#)
- [KEK CA Certificate](#)
- [CRL](#)
- [KEK CA Signing Policy](#)

Powered by NAREGI CA Ver1.0 User Enroll Service.



KEK CA WEB User Enroll - Microsoft Internet Explorer

http://192.168.48.201/testca_ra/a/enroll?Op=UserNewCert

大学共同利用機関法人
KEK
高エネルギー加速器研究機構

Requesting a certificate to the CA server.
Please fill out application form, and click [Request a certificate] button.

User Enroll Service

Request form

Group Information

Group Name : **SMIME user**

User Information

User Name :

Email :

Email(confirm) :

User Private Key

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Length: 512 bit 1024 bit 2048 bit

Key Export: Exportable NOT Exportable

Key Save Level: Normal Level Higher Security Level

* Long key length (ex. 2048 bit) may not be used. It depends on specified CSP.

[Change Password](#) | [Logout](#)

Powered by NAREGI CA Ver1.0 User Enroll Service.

ページが表示されました

インターネット

staffing

- User Administrator
 - Mitsue Arai and Yumiko Kimura as receptionist
 - Takashi Sasaki
- Security officer
 - Kohki Ishikawa
 - Yoshimi Iida
- CA operator
 - TBA
- Help Desk
 - CRC Help Desk

